GDOT Publications
Policies & Procedures

Policy: 8010-3- User Responsibilities and Acknowledgements to the Computer Information Systems Policy
Section: EDP Procurement
Office/Department: Information Technology
Reports To: Deputy Commissioner
Contact: 404-631-1000

PURPOSE

GDOT information technology resources are provided to authorized users to facilitate the efficient and effective performance of their duties. It is the responsibility of Users to ensure that such resources are not misused. Policy has been established in order to:

- Comply with Federal and state laws and regulations regarding information security.
- Safeguard the systems and information contained within these systems.
- Reduce business and legal risk.

SCOPE

The policy applies to employees, contractors, consultants, temporaries, and other workers (hereafter collectively referred to as users) at all facilities of the Department of Transportation, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by DOT or is connected to the Department's network. Users who utilize the Department's electronic infrastructure should familiarize themselves with their responsibilities and acknowledgments prior to signing the Computer Information Systems Policy User Responsibility Agreement form, DOT 1801.

RESPONSIBILITY

1. The IT Director/CIO retains authority for enforcement and monitoring of this policy.
2. The IT Director/CIO is responsible for designating a person to serve this function in case of absence or emergency.
3. The Administrator of the IT Office of Infrastructure is responsible for compliance with the policy, updates to the policy, monitoring, and enforcing the policy.
4. In the absence of the IT Office of Infrastructure administrator, the Assistant Administrator of Infrastructure is responsible for compliance with the policy and for reporting concerns to the IT Director/Chief Information Officer.

SUPPORTING DOCUMENTS

Doc ID	Title	Description	Effective date
GTA Policy No. P-08-003.01	Security Policies & Communications and Operations Management	Appropriate Use of Information Technology Resources	03/20/2008

GTA Standard No. S-08-001.01	Communications and Operations Management	Appropriate Use and Monitoring	03/31/2008
GTA Standard No. S-08-009.01	Communications and Operations Management	Electronic Communications Accountability	03/31/2008
GTA Standard No. S-08-011.01	Communications and Operations Management	Email Use and Protection	03/31/2008
GDOT Policy 2255-1	Standards of Conduct	Standards of Conduct	reviewed: 06/08/07
GDOT Policy 8010-2	Computer Information Systems Policy	Comply with Federal and state laws and regulations regarding information security	reviewed: 06/08/07
GDOT Policy 8005-1	IT Email Use and Retention Policy	Standards for the proper use of Email services provided by the GDOT	6/7/2010

DEFINITIONS

Information Technology Resources or IT Resources applies to hardware, software, and communications equipment, including, but not limited to:

- Personal computer
- Email
- Internet
- Mainframes
- Wide and local area networks Servers
- Mobile or portable computers Peripheral equipment
- Telephones Wireless communications Facsimile machines

Technology facilities (including but not limited to: data centers, dedicated training facilities, and switching facilities) and other relevant hardware/software items as well as personnel tasked with the planning, implementation, and support of technology.

Inappropriate usage includes (but is not limited to) actual or attempted misuse of information technology resources for: Conducting private or personal for-profit activities. This includes use for private purposes such as business transactions, private advertising of products or services, and any activity meant to foster personal gain Conducting unauthorized not-for-profit business activities Viewing pornographic materials Conducting any illegal activities as defined by federal, state, and local laws or regulations Creation, accessing or transmitting sexually explicit, obscene, or pornographic material Creation, accessing or transmitting material that could

be considered discriminatory, offensive, threatening, harassing, or intimidating Creation, accessing, or participation in online gambling Infringement of any copyright, trademark, patent or other intellectual property rights Performing any activity that could cause the loss, corruption of or prevention of rightful access to data or the degradation of system/network performance Conducting any activity or solicitation for political or religious causes Unauthorized distribution of state data and information Attempts to subvert the security of any state or other network or network resources Use of another employee's access for any reason unless explicitly authorized Attempts to modify or remove computer equipment, software, or peripherals without proper authorization Attempts to libel or otherwise defame any person.

Authorization and need-to-know is above and beyond the administrative approval needed to access sensitive information. In addition to having the formal approval to access information, individuals must also have system authorization and a need, based on their job functions or role to access the information. (Example: GDOT system administrators have administrative approval for privileged access to the GDOT intranet, however, based on their job functions they are not authorized nor do they have a need-to-know the information contained in personnel files)

Data Custodianship is the responsibility assumed by anyone entrusted with GDOT information for upholding the security objectives of confidentiality, integrity and availability while that information is in that person's possession either physically or digitally.

Electronic Mail (email) is a method of composing, sending, storing, and receiving messages over electronic communication systems or email systems. The term "email" applies both to the Internet email system based on the Simple Mail Transfer Protocol (SMTP) and to intranet systems allowing users within one company or organization to send messages to each other.

Email Systems are software and hardware systems that transport messages from one computer user to another. Email systems range in scope and size from a local email system that carries messages to users within an agency or office over a local area network (LAN) or an enterprise-wide email system that carries messages to various users in various physical locations over a wide area network (WAN) email system to an email system that sends and receives messages around the world over the internet. Often the same email system serves all three functions.

Email Messages are electronic documents created and sent or received by a computer via an email system. This definition applies equally to the contents of the communication, the transactional information, and any attachments associated with such communication. Email messages are similar to other forms of communicated messages, such as correspondence, memoranda, and circular letters.

POLICY STATEMENTS

GDOT information technology resources are tools to be used to facilitate the execution of official state business. The use of such resources is subject to state government policies and applicable state and federal laws. Users of State information technology resources shall refrain from inappropriate use (as defined in Terms and Definitions) of such resources at all times, including during breaks or outside of regular business hours. Department of Transportation (DOT) electronic infrastructure users must agree to comply with the following responsibilities and acknowledgments:

A. Appropriate Use and Monitoring

1. GDOT information technology resources are to be used to conduct official state business. Occasional use of GDOT Internet and email for non-work related reasons is permitted so long as it doesn't involve inappropriate use as described in existing policies 8010-3, 8005-1, and 8010-2. Any such use should be brief, infrequent, and shall not interfere with User's performance, duties and responsibilities. All activity is monitored and subject to review at any time. This privilege may, however, be withdrawn if abused.

2. Users of GDOT information technology resources shall assume NO expectation of personal privacy outside protections provided by the Privacy Act or 1974, HIPAA, and/or other federal, state, or local regulations.
3. All information created, transmitted, and stored on GDOT information technology resources is the sole property of the GDOT and is subject to monitoring, review, and seizure.
4. Logging on to GDOT information system is an acknowledgement of this standard and an agreement to abide by it and all other governance regarding its use.
5. GDOT shall provide notice of the right and intent to monitor by displaying an Appropriate Use Banner on all computers.

B. Electronic Communications Accountability
1. All electronic communications generated from a GDOT Information System or in connection with conducting state business must adhere to the IT Policies and Standards for Appropriate Use.
2. Anyone in possession of GDOT information assets assumes custodial responsibilities of the information.
3. All electronically stored information that's owned or controlled by GDOT shall be managed by its internal procedures for appropriate handling and storage.
4. Originators of electronic data or correspondence are responsible for appropriateness of message content, awareness of data classification, and confirming authorization and need-to-know of the recipients before transmitting any electronic correspondence from a GDOT information system on behalf of the GDOT.
5. Upon forwarding information, the individual forwarding assumes responsibility as an originator (above) for proper handling and disposition of the information.

C. User Responsibilities and Acknowledgments Department of Transportation (DOT) electronic infrastructure users must agree to comply with the following responsibilities and acknowledgments:
1. Acknowledge that the Department's electronic infrastructure is designed for Departmental business use and that communications are for the purpose of carrying out the professional responsibilities of employees or contractors/consultants of the DOT.
2. Take all necessary steps to prevent unauthorized access to sensitive, non-public Department information.
3. Take all reasonable precautions to protect computer hardware, software, data, documentation and information from misuse, theft, unauthorized access, and environmental hazards including disposing of any unneeded media containing sensitive information in an approved secure manner.
4. Keep passwords secure and do not use another's identity or password. Authorized users are responsible for the security of their passwords and accounts and for all transactions made with their user id and password. User level passwords must be changed on a monthly basis. Secure all PCs, laptops and workstations with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (or control- alt-delete screen lock for Win2K users) when the host will be unattended.
5. Do not perform equipment installations, disconnections, modifications, and relocations without written consent from the Division of Information Technology (IT) or the District Systems Support. This does not apply to temporary moves of portable computers for which an initial connection has been set up by IT.
6. Do not copy, download, install or run software unless authorized by IT. Only software that is licensed to or owned by the DOT should be installed or run on its computers. All other software is prohibited.

7. Do not take shared portable equipment such as laptop computers out of the office without the informed consent of your supervisor. Informed consent means that your supervisor knows what equipment is leaving, what data is on it, for what purpose it will be used and when is its expected returned time.
8. Utilize non-Department equipment to access the Department network only after receiving approval by the appropriate Office Head, District Engineer or Division Director and meeting security requirements specified by IT in the Computer Information Systems Policy.
9. Do not use a DOT email address to post non-DOT information to news groups or to sign up for non-DOT business related emailing.
10. Be responsible for the content of all text, audio, or images that is placed or sent via email. All external communications shall include the user's name, title, division, office/company, and phone number as a signature. Example:

    John Q. Smith John M. Doe
    State Employee Consultant
    Division of Whatever DOT Office - Contract is with
    Office of Something ABC Consulting Company
    404-123-4567/404-123-4567

11. Do not include verbiage or graphics in email signatures that violate State or Federal Regulations.
12. Do not intentionally violate copyright laws by transmitting copyrighted materials without permission.
13. Do not send or voluntarily acquire any sexually explicit or sexually oriented material, hate-based material, hacker-related material or other material determined by the Department to be off limits through DOT Intranet or Internet. These materials cannot be stored on your assigned DOT computer's hard drive or personal share.
14. Do not perform any act that may defame, libel, abuse, embarrass, tarnish, present a bad image of, or portray in false light, the DOT or any person.
15. Acknowledge that child pornography violates Federal law and any violation shall be reported to law enforcement authorities.
16. Avoid transmission of sensitive or non-public information. If it is necessary to transmit such information, users shall obtain authorization from the appropriate Division Director prior to doing so and take the necessary steps required to ensure that information is delivered to the proper person who is authorized to receive such information for legitimate use.
17. Do not browse private files or accounts of others, except as authorized by the network account user except for IT personnel with the appropriate security clearance.
18. Do not perform any activities that circumvent security or access controls of the infrastructure of the Department or any other organization, including the possession or use of hardware or software tools intended to defeat software copy protection, discover passwords, identify security vulnerabilities, decrypt encrypted files, or compromise network or information security by any other means.
19. Unless authorized in writing by your Office Head, Division Director or District Engineer, do not use any services available on the Internet, such as FTP or Telnet, on systems for which the user does not have an account, or on systems that have no guest or anonymous account for the service being used.
20. Do not knowingly introduce any computer infecting agents into Department computers or load diskettes/CDs/DVDs, jump drives and/or any other removable storage devices of unknown origin.

21. Take normal user precaution that the antiviral protection on any machine being connected to DOT's network is up to date and operating properly. At a minimum a user should comply with messages recommending antiviral software updates and report to the Solutions Center or your District Systems Support person when an error or infecting agent notification message appears.
22. IMMEDIATELY POWER OFF the workstation and contact either their local Support Administrator or the Solutions Center at 404-631-1220 if you suspect that a virus has infected your workstation.
23. Acknowledge that DOT reserves the right to access and review anything created and/or stored on Department systems without user consent
24. Mass distribution of an electronic mail is restricted to purposes related to the Department's mission of public service to the citizens of the State of Georgia. Mass distribution must be approved by your Office Administrator, Division Director or District Engineer.

Acknowledge that employees who violate the Computer Information Systems Policy are subject to appropriate disciplinary action up to and including termination of employment.

Acknowledge that users who violate the Computer Information Systems Policy are subject to losing access to the Department's electronic infrastructure.

References:

Computer Information Systems Policy, 8010-2
Computer Information Systems Policy User Responsibility Agreement form, DOT1801

History:

Updated content on 8/13/13
Reviewed: 8/27/2013